CLAIMS

What is claimed is:

1. A secure storage device for storing and retrieving information in response to storage or retrieval commands, comprising:

an interface for receiving the commands and information;

a cryptographic processor for performing data encryption and decryption, wherein the data encryption includes a two-way encryption process which produces encrypted data when applied to the data and a one-way process which produces at least one initial check value when applied to the data, and wherein the decryption utilizes the two-way encryption process to produce data and the one-way decryption process to produce at least one decrypted data check value, wherein the decrypted data will not be transferred unless the at least one initial check value and the at least one decrypted data check value match; and

a storage system, including a storage medium, for the storage and retrieval of the encrypted data and at least one initial check value.

2. The secure storage device of claim 1 wherein the two-way encryption process is a Rijndael algorithm.

3. The secure storage device of claim 1 wherein the storage or retrieval commands include a cryptographic key.

4. The secure storage device of claim 1 wherein the initial check value and the decryption value are 4 bytes long.

5. The secure storage device of claim 1 wherein the cryptographic processor can be disabled.

6. The secure storage device of claim 3 wherein the one-way processes produces the initial check value and the decryption check value by applying a hash algorithm which utilizes the cryptographic key.

7. The secure storage device of claim 1 wherein the storage device is an optical disc drive and wherein the storage medium is a removable storage disc.

8. The secure storage device of claim 1 wherein the interface is a SCSI interface.

9. The secure storage device of claim 1 wherein the interface is a communication bus.

10. The secure storage device of claim 1 wherein the cryptographic processor comprises an encryption chip and a decryption chip.

11. The secure storage device of claim 10 wherein the encryption chip and the decryption chips are programmable logic devices.

12. The secure storage device of claim 10 wherein the encryption chip and the decryption chips are each an ASIC.

13. The secure storage device of claim 1 wherein the storage system stores both the encrypted data and initial check value on the storage medium.

14. The secure storage device of claim 13 wherein the storage system retrieve both the encrypted data and the initial check value during the retrieval of information so that the initial check value can be compared against the generated decryption check value.

15. A method of securely storing data in a data storage device in response to a storage request so that the securely stored data cannot be retrieved without authorization, comprising:

(a) receiving data to be stored and an encryption key from the host computer;

(b) encrypting the data using a two way encryption process and the encryption key;

(c) generating an initial decryption check value using a one way encryption process and the encryption key; and

(d) storing the encrypted data and the initial decryption check, thus providing the capability to prevent the retrieval of information unless the initial decryption check value matches a later generated decryption check value.

16. The method of securely storing data of claim 15 wherein the later generated decryption check value is generated by decrypting the encrypted data using the two way encryption process and a decryption key to produce decrypted data, and applying the decrypted data and the decryption key to the one way encryption process, thus producing the later generated decryption check value.

17. The method of securely storing data of claim 16 wherein the decryption key is provided as part of a request for retrieval.

18. A method of retrieving securely stored data which includes encrypted data and an initial decryption check value in response to a retrieval request, comprising:

(a) retrieving the encrypted data and the initial decryption check value;

(b) decrypting the encrypted data using a two way encryption process which was also used to encrypt the data and a decryption key supplied as part of the retrieval request;

(c) generating a second decryption check value by applying the decrypted data and the decryption key to a one way encryption process; and

(d) providing the decrypted data if the initial decryption check value and the second decryption check value are equal.

19. The method of retrieving securely stored data of claim 18 wherein the decryption key is provided as part of a request for retrieval.

20. A method for the secure storage and retrieval of data in a storage device, comprising:

(a) receiving data to be stored and an encryption key;

(b) encrypting the data using a two way encryption process and the encryption key;

(c) generating an initial decryption check value using a one way encryption process and the encryption key;

(d) storing the encrypted data and the initial decryption check, thus providing the capability to prevent the unauthorized retrieval of information unless the initial decryption check value matches a later generated second decryption check value;

(e) in response to a request for retrieval which includes a decryption key, retrieving the encrypted data and the initial decryption check value;

(f) decrypting the encrypted data using the two way encryption and the decryption key provided in the request for retrieval;

(g) generating the second decryption check value by applying the decrypted data and the decryption key to the one way encryption process; and

(h) providing the decrypted data if the initial decryption check value and the second decryption check value are equal.